STATEMENT

OF

HARRIS MILLER

President

Information Technology Association of America

BEFORE THE

HOUSE COMMITTEE ON GOVERNMENT REFORM

CONCERNING THE IMPLEMENTATION OF THE "SUPPORT ANTI-TERRORISM BY FOSTERING EFFECTIVE TECHNOLOGIES ACT OF 2002"

ON BEHALF OF

INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

October 17, 2003

Introduction

Mr. Chairman and Members of the Committee. Thank you for inviting the Information Technology Association of America (ITAA) to testify today on the Department of Homeland Security's proposed and interim final regulations to implement the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act), which was passed as part of last year's landmark legislation creating the new Department of Homeland Security ("DHS," or "the Department"). The SAFETY Act, as this portion of the legislation is known, is intended to facilitate the rapid development and deployment of technologies and services that offer remarkable potential to improve the security of the American people.

My name is Harris Miller, and I serve as President at ITAA. ITAA is the nation's leading and oldest trade association focused on the diverse information technology (IT) industry, and provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of more than 400 corporate members throughout the United States, and serves as the Secretariat for the World Information Technology and Services Alliance (WITSA), a global network of 50 countries' national IT trade associations. ITAA represents virtually every major federal contractor and many other public and private sector contractors, and counts among its membership a wide range of companies from the largest enterprise solutions providers to the smallest IT start-ups. The Association takes the leading role in major public policy issues of concern to the IT industry, including government IT procurement, homeland security, information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy protection, and e-commerce, among others. Of particular note to this hearing, ITAA also serves as the co-sector Coordinator for the ICT sector, as designated by DHS.

As the nation mobilizes to respond to new asymmetrical threats, the federal government has recognized the need to access America's technological resources to safeguard the homeland against future acts of terrorism. No one wants to wake up the day following another terrorist attack like the one our nation suffered on September 11, 2001 with the knowledge that we could have done more to prevent it. At the same time, the use of technology to secure the homeland carries with it significant risk of potentially unbounded and uninsurable

liability in the event of a terrorist attack where anti-terrorism technology was deployed to prevent such an event. The SAFETY Act seeks to strike a balance between the potential and the risk of deploying technology to defend against terrorism by establishing a regime to mitigate the technology providers' exposure to liability for potentially catastrophic losses resulting from acts of terrorism that could circumvent even the most innovative technology designed to prevent them. It is important to note that the SAFETY Act doesn't just protect sellers; entities that are mandated to implement anti-terrorism solutions also require protection, and the SAFETYT Act affords protection to those entities as well.

Passage of the SAFETY Act was a critical first step towards ensuring that U.S. citizens would have access to the benefits of the full range of technology solutions to aid in the war on terrorism. With passage of the statute, the focus necessarily shifted to implementation and ITAA began working with the Department and the Office of Management and Budget (OMB) to accomplish this objective as quickly as possible. I would like the record to show that ITAA strongly supports the Department's general approach to implementing the SAFETY Act that has been reflected in both the proposed regulations published on July 11, 2003 and in the interim final regulations that were published yesterday in the *Federal Register*. In particular, we are pleased that the Department's regulations carry out the statutory distinction between designation of products and services as qualified anti-terrorism technologies (QATT), and those QATT that are further certified as approved products for purposes of the government contractor defense. ITAA was also pleased to see that the Department interprets the statute to provide for a single federal cause of action that may only be brought against the "Seller" of the QATT. We also appreciate the Department's candid and open request for constructive suggestions about a range of significant policy issues.

Having said all that, ITAA does still have a number of both policy and process concerns that we raised first in response to the proposed regulations and that have carried over in reaction to the interim final regulations and the Department's implementation of the SAFETY Act more broadly. The remainder of our testimony today will focus on these concerns.

When the Department published it's NPRM in the *Federal Register* on July 11, it provided for a 30-day comment period for interested parties to respond. ITAA joined with several other leading trade associations in submitting extensive and detailed comments on the proposed regulations. At least forty-nine other entities submitted comments to the Department, many of which were equally detailed and also raised significant concerns with substantive issues that must be resolved prior to final implementation of the statute.

I provide for the record a copy of the comments ITAA submitted along with the Professional Services Council, the Aerospace Industries Association, and the National Association of Manufacturers. Because of the length and breadth of our

joint comments, our testimony today will focus more broadly on issues of concern to the IT community. I would refer you to our formal comments to the proposed regulations for our detailed analysis of the draft regulations. Our industry colleagues from the Professional Services Council (PSC) and U.S. Chamber of Commerce will address other areas of concern to the private sector.

In the initial "Regulatory Background and Analysis" section of the NPRM that prefaced the actual text of the proposed regulations (the "Preamble"), DHS indicated that the Department would begin accepting applications for QATT designation and approved product certification on September 1, and that the forms of application necessary to initiate these processes would be posted on the official DHS website. Many in industry were dubious of this timetable since the September 1 deadline – which was itself a federal holiday – allowed only **two weeks** from the expiration of the comment period for DHS to review and address comments on a major regulatory initiative. Moreover, in the absence of the application forms or any other information in the proposed regulations about the content of applications or the specific information required to be submitted, industry was left to respond in many ways in the abstract to the proposed rules. ITAA's comments in particular, though detailed as to the provisions outlined in the Preamble and proposed regulations, were hypothetical in nature since the application forms were not published.

On September 8, 2003, DHS published an emergency request for clearance of an information collection request to OMB in the *Federal Register*. This clearance request focused on what DHS is terming the "Application Kit" that interested vendors will use to apply for designation and/or certification under the terms of the SAFETY Act. ITAA obtained a copy of the supporting materials sent over to OMB—namely the application kit—and has been astounded at the kinds and scope of information to be required of applicants. We will discuss in more detail the concerns we have with the data being requested by DHS, but want to begin with an overview of the concerns industry has about the forms.

We cannot overemphasize the importance of the scope and content of the application forms. Until industry sees the actual final application forms the Department plans to use, we cannot be certain of the appropriateness of the information to be collected or the real burdens applying for designation and/or certification will that will be placed on companies seeking either approval from the Department. Industry needs to have input into the scope and form of the final applications, and we urge DHS to reach out to the industry community to seek input and comments on the draft applications as soon as possible. Now that the interim final rules have been published and the regulatory framework is effective, ITAA members want to know how and in what form they should submit applications to the Department for certification and/or designation. In the absence of an approved application kit, we believe there will be countless efforts undertaken by interested parties that may be rejected by the Department as a result of some gap in information contemplated in the proposed applications.

DHS's self-imposed deadline of September 1 has come and gone, and the Department has not yet released a draft of the application. Because of the nature and scope of information contemplated in the draft application submitted to OMB, ITAA believes it is critical for the Department to afford industry the opportunity to provide comments before using the proposed forms to process applications.

Yet even in the absence of the actual form, DHS has indicated to the vendor community in a variety of fora that it will accept submissions for certification and/or designation prior to the finalization of application kit. The Department recently posted a new SAFETY Act web page within its web site. The site notes in part that "Individuals may submit technologies for consideration to: Department of Homeland Security, Attn: SAFETY Act, 245 Murray Lane, Building 410, Washington, DC 20528." The site goes on further to indicate "at a future date, the Department will issue a formal application and submission criteria. Therefore, the Department reserves the right to request further information from submitters who request SAFETY Act consideration prior to the release of the formal application process."

This statement would seem to imply that companies seeking Departmental review of technologies may submit information to the Department prior to the release of the formal applications for designation and certification. ITAA is concerned that the language included on this website will lead to a flurry of submissions to the Department, and that in the absence of a formal process, DHS will be inundated with submissions that require formal evaluation criteria. Given that the regulatory framework is now effective as of yesterday, the lack of an approved application form is of even greater concern. We urge the Department to clarify the information on its website to assure that the designation and certification process works expeditiously for the benefit of both the government and its suppliers.

DHS just this week finished a series of informational "road shows" designed to educate the business community about the SAFETY Act and the specific application procedures for designation and certification under the Act. ITAA attended the first of these sessions on in late September in Dallas and had either staff or member representatives at each of the other forums held around the country, including the most recent event held in Washington on Tuesday of this week. Based upon the presentations given at the road shows and the supporting information in the application kit submitted to OMB, there are several concerns that we have about the Department's interpretation of the SAFETY Act statute and the amount and scope of information to be required for applications to the Department.

At the forums, DHS outlined significant data requirements for parties interested in receiving designation and/or certification of anti-terrorism technologies that quite

frankly were not even conceived of in the proposed regulations or enumerated in the interim final rule. ITAA is concerned that the massive scope of scientific, business, and insurance/risk data to be required on applications to the Department is so burdensome that even the largest information technology companies will need to assemble massive internal teams to comply with the requirements. While the scope and amount of data to be submitted to DHS may be assembled in large enterprises, we have significant concerns about the ability of smaller companies to comply with the information requirements outlined by the Department. Among other pieces of information, DHS envisions requiring applicants to submit information on the profitability of the technology, significant self-insurance data and virtually any conceivable technical data relating to a particular technology. ITAA will provide comments to the Department and to OMB on the burden estimates outlined in the interim final rules. Let me just state for this committee that based on feedback provided by ITAA members, we believe the Department has grossly underestimated the burdens applications will place on applicants.

We are concerned that the technical and business evaluation information requirements are so massive as to ignore the real-world business issues surrounding deployment of anti-terrorism technologies and urge the Department to rethink the scope of information to be required on applications. Based on the information presented at the forums, we are concerned that the regulations and information to be required on applications are so complex and so burdensome that they may themselves serve as a severe impediment to the deployment of anti-terrorism technologies and services. We are also concerned that the Department has not clearly identified how it specifically will protect this sensitive proprietary data from unauthorized disclosure or dissemination. At the SAFETY Act road shows, the Department indicated it's strong preference for electronic submission of applications and supporting data. While ITAA will certainly be the first to support and embrace the power of the internet to enhance and transform business processes, the Internet is still an open system and is vulnerable to breaches. We are concerned that there is no mention of a comprehensive management plan to secure the systems over which data will be transmitted, policies and procedures applicable to DHS personnel operating and having access to the system, or details on the technological approaches the Department will take to secure the data provided by applicants. We urge the Department to work with industry to develop and implement a comprehensive plan to secure the data and network over which this highly sensitive, proprietary information will flow.

Additionally, DHS outlined at the forums and has noted in its interim final rules the availability of an optional "pre-application" process whereby firms can submit condensed information to the Department to receive feedback on the likelihood of a full-blown application receiving certification and/or designation. ITAA understands and appreciates the spirit of this pre-application process, but is concerned that a pre-application program would further elongate an already

extensive review process. We are also concerned about the Department pre-judging technologies and services without full disclosure of information required in a full application.

DHS also maintains that SAFETY Act coverage is envisioned only for the narrowest of technologies specifically designed for anti-terrorism applications. The Department has also been quoted in recent news stories as interpreting the SAFETY Act to apply only to "new" technologies developed specifically for homeland security applications. While we understand that the Department has backed away from this interpretation of the statute, we are nevertheless extremely concerned that the Department interprets the SAFETY Act to apply to such a limited scope of technologies and services. The SAFETY Act statute makes no reference to technologies exclusively "designed" for anti-terrorism applications, but rather, references that coverage be extended to technologies and services "designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary." ITAA believes that a wide array of technologies not originally developed with specific anti-terrorism applications in mind will nevertheless have wide applicability in the homeland security arena, and we urge the department to clarify in its final regulations and application/briefing materials that the SAFETY Act applies to all manner of technologies that may be procured for homeland security purposes as the statute specifies. We address this issue in additional detail below.

Overview of ITAA Comments on the SAFETY Act Regulations

ITAA's comments to DHS on the proposed regulations address a wider range of issues than we can detail in this statement, and I would commend them to the Committee for a detailed position of ITAA on the changes needed to the proposed regulations. As noted earlier, they are attached.

Today I would like to focus our testimony on several broad issue areas that were addressed in our comments and remain of concern now that the interim final rule has been published. These concerns center around:

- The need for an expedited process for priority procurements;
- The time-frame for designation and certification of QATTs under the proposed regulatory framework;
- The need for sufficient flexibility in the scope of QATT designations and approved product certifications to ensure complex IT product and/or service offerings are properly addressed;
- Insurance provisions of the proposed rule;
- Issues associated with the single federal cause of action;

- Concerns with provisions dealing with post-designation and certification changes to approved products and services;
- Procedures to ensure the confidentiality of information submitted as part of applications for designation and/or certification;
- Appeal procedures for denials of applications for designation and certification; and
- The relationship between the SAFETY Act and indemnification under Public Law 85-804.

The Need for an Expedited Process for Priority Procurements

Whether and how quickly a technology is designated and/or certified under the SAFETY Act will have a profound impact on the acquisition of technology and services to fight the war on terrorism. While we are pleased that the Department indicates in the interim final rule that it will work to prioritize reviews, there is no clear standard outlined as to how the Department plans to accomplish this prioritization. There is also no clear framework for how DHS plans to prioritize reviews for technologies of interest to agencies other than DHS that have a need to acquire QATTs.

ITAA believes that the final regulations should be amended to expressly accommodate the needs of other agencies that will acquire technologies and services designed to fight the war on terror. Specifically, we believe that the regulations should provide that federal, state, and local agencies may notify offerors that a particular solicitation contemplates the acquisition of technology that will be recommended to DHS for designation as a QATT.

As noted above, while the Department has acknowledged that it intends to prioritize reviews based on the most immediate needs, we believe the final regulations should provide for an explicit mechanism to prioritize and expedite certain applications. ITAA strongly believes that what is most urgently needed right now is an appropriate process for expediting treatment of procurements that are ready to move forward and where the need for immediate deployment is urgent and compelling. This expedited process should apply not only to federal acquisitions of anti-terrorism technology, but to priority non-federal procurements as well – particularly, procurements by state and local authorities with frontline homeland security responsibilities for protecting critical infrastructure that is high on the Department's threat matrix. There are many procurements that have been awaiting resolution of liability concerns provided by the protections afforded under the SAFETY Act. Some of these procurements involve securing ports, bridges, mail services and other facilities critical to our nation's security. The expedited process should include a provision requiring that SAFETY Act review be performed in tandem with the agency's proposal evaluation process to the maximum extent possible.

In addition, the interim final regulations are silent on many other comments in the procurement arena that were provided by ITAA and other groups in response to the proposed regulations. Specifically, we believe the regulations should encourage agencies to allow the submission of (1) bids or proposals for which the price, contract performance, or other terms are conditioned upon QATT designation; (2) bids or proposals in which the bidder reserves the right to withdraw the bid or proposal if QATT designation is not received, or (3) bids or proposals which are conditioned upon a price renegotiation if QATT designation is not received or an insurance requirement is set at a higher cost than was set forth as a stated assumption in the bid or proposal. QATT designation will make a material difference in many procurement contexts and the issues surrounding it should be treated with this kind of flexibility. We believe that corresponding revisions to the FAR should be pursued to make this requirement binding upon other government agencies.
There is no clear discussion of these issues in the interim final rule and we urge the Department to amend the regulations to address these issues explicitly.

Marketplace pressures continue to mount against contractors with either existing technologies capable of contributing to the war on terrorism, or technologies in development, to deliver these products and services to the federal government. Absent the protections promised by the SAFETY Act, we are concerned that contractors will not be able to respond to critical needs. We appreciate the Department's acknowledgement that it will work to prioritize reviews and urge the Department to provide in the final rules the greatest flexibility necessary to prioritize the reviews required for designation and certification, both with respect to on-going or planned procurements, and to critical technology needs for which the Department requires innovative technologies and services.

Issues Concerning the Designation/Certification Timeframe

ITAA is still concerned that the interim final rules contemplate a minimum 150-day period for the designation/certification process to run its course. In light of the urgent needs that exist today, a lengthy approval process timeframe could complicate the rapid development and deployment of QATT. More importantly, it is critical that the final regulations provide for an expedited approval process for the review of technologies already in use or substantially equivalent to existing QATTs, changes and modifications to existing QATTs, technologies that are the subject of pending procurements for the protection of high-risk targets or critical infrastructure, technologies for which the cost of insurance has changed significantly, and in other appropriate circumstances.

The draft regulations proposed and the interim final rule maintains an across-the-board term of five to eight years on all designations of QATT. Because DHS does not explain its rationale for establishing a mandatory expiration date, it is difficult to weigh the pros and cons of such a requirement. ITAA believes that an

automatic expiration date for every designation, regardless of the circumstances, will tend to discourage the development of anti-terrorism technology because the seller would know that a designation, even if granted, would be effective only for a limited period of time. We are also concerned that an arbitrary timeframe for designation would needlessly increase costs for both sellers and the Department; sellers would have to build costs for renewal of designations into their cost structures, and the Department would have to review such applications every five to eight years, even when there have been no material changes to the technology or service.

The SAFETY Act, as passed by Congress and signed into law by the President, provides no term for a designation under the SAFETY Act. ITAA believes very strongly that the regulations should require that designations will apply for an indefinite period. Changes in technology that would require re-approval of the designation/certification are addressed in other areas of the proposed and interim final regulations, and absent any material changes in the technology or the insurance covering the technology or service, the approval should extend indefinitely.

If the final regulations are to require some term for an effective designation, we believe that DHS should explicitly substantiate why the 5 to 8 year period is needed absent a legislative requirement in this arena. In that case, we also believe that the timeframe should be extended to a minimum of 10 years—if not substantially longer—which is more consistent with the effective dates of long-term services agreements and more realistically reflects the length of time necessary to develop and implement complex systems and services.

ITAA also has concerns with the interim final rule's determination that designation/certification will be effective on the date of issuance by the Department. ITAA believes that the regulations should provide that a designation and/or certification should take effect retroactively to the earlier of the date of deployment or the date of sales. The regulations should also state that once designation/certification is obtained, the liability protections of the SAFETY Act will apply even if the facts of a particular claim are alleged to have occurred prior to the effective date of the designation/certification. By providing protection to a seller who elects to make its technology immediately available to the public pending the DHS approval process, retroactive designation and certification would encourage the deployment of a QATT at the earliest possible date.

At an absolute minimum, a designation/certification granted by the Department should be retroactive to the date of application. Moreover, any effective date should be outlined in the approval certificate issued by DHS rather than in the regulations themselves.

Need for Broad Scope of QATT Designations and Approved Product Certifications

Members of this Committee led the charge during consideration of the SAFETY Act to include anti-terrorism services in the scope of items to be covered by designation and/or certification. Anti-terrorism services are as critical to security as anti-terrorism technologies and devices, and, given the wide variations in the complexity of such services, are likely to require much more flexibility in the regulatory review process. We're happy that the services industry is also represented on this panel by the Professional Services Council. I am certain you will hear much more about the critical role services play in the anti-terrorism arena. On behalf of the information technology service providers, we stress that the regulations should clearly provide that designations and certifications of QATTs are sufficiently broad to include all elements of the component products and services, including systems design and customer-approved changes and related services, such as operations, maintenance, integration, and training. We are also concerned that the regulations do not adequately address the need to cover the range of deliverables across the entire spectrum of a procurement; complex system integration services, for example, could include a range of employee training, maintenance, and upgrade services might be offered that could be beyond the traditional scope of a technology designation or certification.

DHS maintains that services will be provided the same treatment as technologies in their reviews by the Department. The interim final regulations stipulate that the same seven criteria will be used to review applications for certification that cover services. As I'm sure our colleagues from the Professional Services Council will discuss, the nature of services is unique and requires greater flexibility in the review and evaluation process. The interim final rules do not adequately address the unique nature of services in this new arena.

We are pleased to see that the interim final rules acknowledge that the Department intends to apply the statute to a broad array of technologies and services, both those under development and already available. Previously, a DHS spokesperson was quoted as saying the protections of the SAFETY Act applied only to new technologies. ITAA strongly objected to this interpretation of the Act and is happy to see that the Department has backed away from this statement.

We are also pleased that the Department acknowledges in the interim final rule that the specific purpose for which technologies are designed does not imply an exclusive purpose. Many technologies with applicability in the war on terrorism may not have been developed with the exclusive purpose of thwarting terrorist attacks, and ITAA is pleased that the Department has recognized this issue.

Insurance Provisions in the Proposed and Interim Final Rule

As provided in the SAFETY Act, the Department's regulations require that the Department be able to certify that, in order to receive QATT designation, the seller has obtained and is maintaining adequate liability insurance for a single act of terrorism to satisfy third party claims where the technology has been deployed. The amount of insurance is not to exceed an amount reasonably available on the world market at prices and terms that would not unreasonably distort the price of the technology or service.

Given the fact that availability of and cost of insurance to satisfy the requirements of the SAFETY Act is uncertain, ITAA believes that the regulations should provide expressly that the Department has the authority to designate/certify technologies or services in the absence of an available policy.

Of particular concern in this area is the statement made by the Department in the interim final rules that in the absence of adequate insurance, the Department may require applicants to self-insure up to an appropriate level of liability determined by the Department. This assertion would seem to run completely contrary to the spirit and intent of the protections envisioned under the SAFETY Act. The genesis of the SAFETY Act began with a known problem of virtually unlimited risks confronting suppliers of anti-terrorism technologies and services. The Department has consistently implied that because the protections afforded under the act are voluntary industry should therefore view coverage as a privilege and accept risks and costs not conceived of in the statute. The reliance on requirements to self insure in the absence of adequate market coverage demonstrates a backwards philosophy within the Department that despite an intense interest by the government in acquiring innovative technologies from the private sector, industry should be willing to incur significant costs and assume incredible amounts of risk to support the war on terrorism. ITAA believes that the final regulations should remove the requirement to self insure and expressly provide that in the absence of available insurance on the open market, the Department will declare an applicant's liability to be zero.

ITAA also believes that given the probable high cost of such insurance coverage compared to current coverage, the costs incurred by a seller for SAFETY Act coverage should be treated as allowable costs under Federal Acquisition Regulation (FAR) § 31.205-28. To eliminate the risk of any dispute on this point, ITAA recommends that the regulations themselves (not the Preamble) be amended to recognize that insurance certified under this section, whether the costs are treated by the contractor as direct costs or indirect costs, shall be considered "insurance required or approved and maintained by the contractor" within the meaning of FAR § 31.205-28(a)(1).

Within the context of insurance, the regulations also require sellers to provide an annual certification to the Department that it has and will maintain the required

insurance, and that sellers notify the Undersecretary for Science & Technology of any changes in the type or amount of insurance coverage for a QATT. There is no such requirement in the statute passed by Congress, and ITAA is concerned that yet another certificate will unnecessarily burden both industry and government. As such, we would recommend that this requirement be deleted from the final regulations.

ITAA shares the concern noted in other comments made to the Department about liability issues surrounding potential terrorist events that occur outside the United States, but which may have economic or other consequences inside this country. We are concerned that the regulations as currently proposed do not address the circumstance in which an act of terrorism involving QATT technologies that take place outside the United States; if a terrorist attack were perpetrated on a target outside the United States despite deployment of designated QATT, it could result in serious economic harm to the United States. We urge the Department to clarify in its final rules that incidents of terrorism occurring outside the United States that involves a QATT technology expressly will receive the same protections envisioned for similar events occurring within our borders. By the same token, the Department's final regulations should make clear that QATT designation and certification is available equally to U.S. sellers and non-U.S. entities that otherwise qualify. The statute makes no distinction. We view this as vital because the fight against terrorism is global and the U.S. Government should extend the protection of the SAFETY Act to sellers to deploy their technology overseas to, either in whole or in part, protect the interest of the United States.

Comments on the Single Federal Cause of Action

The Safety Act states that the United States District Courts "shall have original and exclusive jurisdiction" over suits involving claims relating to acts of terrorism when designated anti-terrorism technology has been deployed, but does not state explicitly that federal actions will preempt litigation in state or local courts.

In the Preamble to the Department's proposed rules, the agency concludes that the "exclusive Federal cause of action" necessarily pre-empts such litigation in non-federal courts, and that such cause of action may be brought only against the seller of the QATT, and not against "arguably less culpable persons or entities, including…contractors, subcontractors, suppliers, vendors, and customers of the [s]eller…." ITAA is generally pleased with the discussion of the single federal cause of action in the preamble to the interim final rules.

The extent to which sellers of designated technologies and their customers and suppliers are kept from being subject to a plethora of lawsuits in various fora is a fundamental premise of the entire QATT program, including most obviously the efficacy of the liability cap keyed to the required level of liability insurance. Given

the importance of this issue, we strongly recommend that the Department codify in a "Findings and Purpose" section of the final regulations themselves the Secretary's understanding of Congressional intent in the SAFETY Act and its resulting overview of the operation of the SAFETY Act program for which the Secretary is responsible, including the inter-relationships among the various sections of the SAFETY Act. Leaving critical matters of interpretation to the Preamble to the rule, rather than codifying such interpretations in the regulations themselves, may lead to confusion among all interested parties. This is true with respect to various issues the Department addresses in the Preamble, but perhaps nowhere is it more important than in this area, which gets to the heart of the protections to be afforded to sellers whose technologies obtain QATT status.

Post-designation and Certification changes to Approved Products and Services

The interim final rule provides for automatic termination of a designation granted by the Department if the technology is significantly changed or modified, including changes in the design, material, manufacturing process or purpose for which a QATT is sold.

In response to the proposed rules published by the Department in July, ITAA noted that it was concerned that if the regulatory process for dealing with changes in qualified technology is overly burdensome it will serve as a disincentive for sellers to make improvements to approved technologies. ITAA believes that only changes that could have an adverse effect on the safety or effectiveness of a QATT would trigger a termination, and we believe the regulations should explicitly provide as such.

ITAA is pleased that the interim final rules have been amended to recognize that a change to an approved QATT will be considered significant only if the change materially affects the function or operation of the QATT, i.e., is detrimental to the safety of the technology or service. It is critical to define as precisely as possible in the final regulations when a change must be submitted to DHS; ITAA believes that the regulations should clarify that upgrades, enhancements, and other changes standard in the particular industry are not subject to additional review, and that the regulations provide for an expedited review of amendments to previously approved QATTs. Because the loss of a QATT designation/certification could be financially ruinous, any ambiguity in the proposed regulations on when a re-submittal is required might lead a seller to conclude that even the most minor changes trigger the requirement to supply additional information to the Department. This would impose significant administrative and financial burdens on the seller, and would result in significant delays in the re-approval of technologies as a result of what we perceive would be a flood of unnecessary filings.

One possible approach to resolving the problem of ambiguity is to provide that the designation for each QATT will be drafted in a way that includes changes approved by the customer and identifies the types of additional changes that will require re-application. As noted above, we believe the regulations should provide the greatest specificity possible on the kinds of changes that will require re-approval. Absent such specificity, ITAA is concerned that every lawsuit involving a QATT will include allegations that the technology was significantly changed and that the original designation was invalidated.

ITAA also believes that the procedures for modifications do not adequately address the nuances of the services environment. The nature and delivery of services may change on a much more frequent basis than the root technology, and the final regulations issued by the Department need to address the specific challenges with upgrades and modifications related to the delivery of services.

Procedures to Ensure the Confidentiality of Information Submitted as Part of Applications for Designation and/or Certification

A substantial portion of the data that a seller is required to disclose to DHS for designation/certification will constitute confidential and proprietary commercial and technical information, including trade secrets. The Department has recognized that "successful implementation of the Act requires that applicants' intellectual property interests and trade secrets remain protected in the application and beyond." The Preamble specifically recognizes the flexibility in the Freedom of Information Act ("FOIA"), but offers no guidance on how it will apply to information submitted in the application process. Id. The regulations also include little guidance for assuring the required protection beyond stating that the application and review process will maintain the confidentiality of an applicant's proprietary information. Section 25.8. We believe that significant modifications to the regulations are essential to assure the protection of proprietary data.

ITAA also believes that the regulations should include specific restrictions on disclosure of (a) information submitted in connection with an application for Designation or Certification, and (b) documents and other materials prepared by Government employees, representatives, or private contractors in connection with the evaluation of applications. The restrictions should explicitly state that the prohibitions in FAR § 3.104-4 are applicable to disclosure of such information if it constitutes "contractor bid or proposal information" or "source selection information" within the meaning of the Procurement Integrity Act, 41 U.S.C. § 423. For information that does not relate to a specific Federal agency procurement, the regulations should include disclosure prohibitions and procedures that are substantially the same as the provisions of FAR § 3.104-4.

Moreover, the regulations should include a rebuttable presumption that information submitted in the application and review process will be deemed to be privileged and confidential "trade secrets and commercial or financial information" exempt from disclosure under the Freedom of Information Act ("FOIA"), regardless of whether the information is marked with proprietary legends and limitations. See 5 U.S.C. § 552(b)(4).

The regulations should also provide that information submitted in the application and review process will be treated as information that "concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association" within the meaning of the Trade Secrets Act, 18 U.S.C. § 1905, regardless of whether the information is marked with proprietary legends and limitations.

The regulations should require DHS in every instance to provide advance notification to the submitter when considering whether to disclose SAFETY Act information to third parties, give the submitter the right to refuse to agree to disclosure of the information, and to seek judicial review of any decision to disclose the information before such disclosure is made.

The broader Homeland Security Act provides that "critical infrastructure information" submitted to DHS – information that is related to the security of critical infrastructure or protected systems -- will be exempt from disclosure under the FOIA. See Homeland Security Act, P.L. 107-296, Section 214(a)(1)(A); 6 U.S.C. 133 (2002). Because much of the information submitted by Sellers may constitute "critical infrastructure information," we suggest that the DHS regulation on confidentiality of information submitted as part of the consultation, Designation, and Certification processes include a cross-reference to the "critical infrastructure information" protections provided by the statute.

The concerns that ITAA has in this arena are magnified as a result of the incredible amounts of data the Department intends to require of applicants. We would note that on the issue of burdens outlined in the interim final rules, there is still a lack of information provided in the rules themselves as to the scope of information required of applicants. In the absence of a discussion of the kinds and amount of data to be required, we believe it will be difficult to provide precise responses to the Department's burden estimates. We urge the Department again to release the draft application kit in a formal way and solicit comments from industry before adopting the application as final.

The Regulations Need to Provide an Appeal Process for Denials of Applications for Designation and Certification

The proposed and interim final regulations provide that the Undersecretary's decisions on designation and certification are final and not subject to review. ITAA is confident that the vast majority of technologies submitted to the Department under these regulations will be highly complex and involve innovative approaches to deter a wide range of chemical, biological, nuclear, and other threats. Given the likely variety and sophistication of these technologies, ITAA believes there is a real risk that significant features may be overlooked or misunderstood during the review and evaluation process, particularly if DHS elects to undertake the review without meeting with the applicant. DHS notes in the preamble to the interim final rule that it believes the review process will be highly interactive, and thus, the need for an administrative review will be unnecessary.

We believe the interests of the government and the public would be best served by a process that builds in a method to resolve uncertainties and correct errors. While the regulations provide for delegation of the authorities afforded to the Secretary under the Act to the Undersecretary for Science & Technology, it would certainly seem appropriate for an applicant to have recourse to appeal to the entity assigned responsibility in the statute for the adoption and enforcement of the Act.

As such, we recommend that the final regulations explicitly provide that the applicant has a right to administrative review by the Secretary of a decision by the Undersecretary to deny or restrict the scope of a designation of technology as QATT or to deny certification of a QATT as an approved product for homeland security. There should be an opportunity for a second look at an application.

Relationship Between SAFETY Act Coverage and Indemnification Under Public Law 85-804

The Preamble to the rule notes that DHS believes "Congress intended that the SAFETY Act's liability protections would substantially reduce the need for the United States to provide indemnification under Public Law 85-804 to sellers of anti-terrorism technologies." At the same time, the Department recognizes that there may be certain circumstances in which SAFETY Act coverage and indemnification under Public Law 85-804 is warranted.

President Bush issued Executive Order 10789 on February 28, 2003, which grants the Secretary of DHS the authority to issue indemnification under Public Law 85-804 and also provides that federal agencies (other than an exception for the Department of Defense) cannot provide indemnification "with respect to any matter that has been, or could be, designated by the Secretary of Homeland Security as a qualified anti-terrorism technology" unless the Secretary of DHS had advised whether SAFETY Act coverage would be appropriate and the

Director of the Office of Management and Budget has approved the use of indemnification.

Both the Preamble and the regulations are silent as to circumstances when indemnification under Public Law 85-804 might be warranted, and the process by which the Secretary will review determinations of other federal agencies to issue indemnification for "any matter that has been, or could be . . . a qualified anti-terrorism technology." We believe that the regulations should include some clarification of these issues.

ITAA recommends that the final regulations provide that designation under the SAFETY Act "shall not" preclude the granting of indemnification under appropriate circumstances. For example, a seller might need indemnification under Public Law 85-804 to protect against damages that might occur if the technology is deployed and there is injury other than that arising from an act of terrorism.

Moreover, ITAA recommends that the regulations clarify that, as part of the process for determining whether SAFETY Act or indemnification under Public Law 85-804 is appropriate, the Secretary of DHS will consult with OMB and other agencies as appropriate but will not exercise a "veto" authority over the determinations of other agencies.

Conclusion

As noted at the beginning of our testimony today, ITAA generally supports the approach taken by the Department in issuing proposed regulations to implement the SAFETY Act. We stand ready to support the Department as it works through the changes suggested by ITAA and many other organizations to ensure that the final regulations provide the best possible framework to ensure the most cutting-edge technologies are available to the Department to support our overarching war on terrorism. Thank you for the opportunity to appear before the Committee today. I would be happy to answer any questions from the Committee.